GuestGate™ Hotspot Gateway
Benutzerhandbuch
Modell 523240





INT-523240-UM-0606-04



Sektion Seite

FCC Regulationen

Elektromagnetische Kompatibilität

Dieses Gerät sendet Radiofrequenzen aus und kann, wenn es nicht korrekt installiert wird, zu schädlichen Interferenzen mit anderen Radiokommunikationsgeräten führen. Es kann jeoch nicht garantiert werden, dass in einer speziellen Installation keine Interferenzen auftreten. Wenn dieses Gerät Interferenzen mit Ihrem Radio- oder Fernsehempfang aufweist, was durch Ein- und Ausschalten des Gerätes festgestellt werden kann, sollten Sie die folgenden Maßnahmen zur Behebung des Problems ausprobieren:

- Positionieren Sie die Antenne neu
- Vergrößern Sie den Abstand zwischen Gerät und Receiver
- Verbinden Sie das Gerät mit einem anderen Anschluss des Receivers
- Wenden Sie sich an Ihren Händler oder einen Radiotechniker
- Stellen Sie sicher, dass Sie abgeschirmte Netzwerkkabel nutzen und so den EMC Standards entsprechen

Dieses Gerät wurde getestet und entspricht den Grenzwerten der Klasse B und der Unterklasse B von Teil 15 der FCC Regeln, welche Interferenz in kommerziellen Umgebungen ausschließen sollen. Der Betrieb dieses Gerätes in einer häuslichen Umgebung kann Interferenzen erzeugen, wobei hier der Anwender dafür verantwortlich ist, dieses Problem zu beheben. Dieses digitale Gerät erfüllt die Anforderungen gemäß der Grenzwerte von Stufe B von EN55022/1998 und die Anforderungen an Immunität gemäß EN55024/1998 für den häuslichen, kommerziellen und Industriebetrieb.

Sicherheit

Dieses Gerät enspricht EN60950 für Informationstechnologie-Geräte.

Radioübertragungsregeln

Dieses Gerät gibt Radiofrequenzenergie aus und muss installiert und betrieben werden mit einer minimalen Distanz von 20cm zwischen dem Gerät und Ihrem Körper.

Dieses Gerät wurde entsprechen der FCC Regeln für den kommerziellen und privaten Gebrauch getestet. Sie müssen sich bei der Installation strikt an die Gebrauchsanweisung halten.

Dieses Gerät enspricht den folgenden Radiofrequenz- und Sicherheitsstandards:

Europa – EU Declaration of Conformity. Dieses Gerät enspricht der Direktive R&TTE Direktive 1999/5/EC mit essentiellen Testläufen wie im Standard EN 301489 (Generelle EMC Anforderungen für Radiozubehör) und ETS 300238 (Technische Anforderungen für Radiozubehör) beschrieben.

USA – Federal Communications Commission (FCC). Dieses Gerät entspricht PTeil15 der FCC Regeln. Der Betrieb des Gerätes unterliegt den folgenden 2 Bedingungen:

1. Dieses Gerät darf keine schädlichen Interferenzen verursachen
2. Das Gerät muss alle Interferenzen akzeptieren, die zu nichtgewolltem Verhalten führen.



1. EINLEITUNG

Herzlichen Glückwunsch für den Kauf eines INTELLINET NETWORK SOLUTIONS™ GuestGate™ HotSpot Gateway. Der GuestGate verbindet Gäste mit Ihrem Netzwerk und erlaubt dabei nur eingeschränkten Zugriff (z.B. Internet, Email, Chat oder andere Programme). Der GuestGate schützt Ihr bestehendes Netzwerk vor unbefugtem Zugriff durch angeschlossene Gastcomputer und schirmt diese, falls gewünscht, sogar untereinander ab. Außerdem unterstützt der GuestGate erweiterte IP PnP (Plug and Play) Technologie: Er stellt sich automatisch auf die TCP/IP Einstellungen des Gastcomputers ein und macht zeitraubendes Rekonfigurieren unnötig. Der GuestGate integriert sich nahtlos in Ihr bestehendes Netzwerk ein und eine weitere Konfiguration des GuestGate ist in den meisten Fällen nicht notwendig.

FUNKTIONSBESCHREIBUNG

Internet Zugang für Gäste

GuestGate wurde hauptsächlich entwickelt um Ihren Gästen einen einfachen Zugang zum Internet ohne zusätzliche Konfiguration zur Verfügung zu stellen. GuestGate nutzt den bestehenden Internetzugang Ihres Netzwerkes um Internet- und Email-Zugriff für Gäste in Konferenzräumen, Hotels oder öffentlichen Plätzen mit WLAN Anbindung zur Verfügung zu stellen. Darüber hinaus schützt GuestGate sicherheitsrelevante Bereiche des bestehenden Netzwerks, indem es keinen Zugriff durch angeschlossene Gastcomputer erlaubt. Kurz gesagt bedeutet das, Gäste haben Zugriff auf das Internet, aber Ihr eigenes Netzwerk, z.B. Ihr File Server, Email- oder Anwendungsserver bleiben verborgen und geschützt.

Passwortgeschützter Internetzugang für Gäste

Ihr Netzwerk Administrator kann für Gäste vorgeben, für den Zugang zum Internet, ein Passwort einzugeben. Dies ist eine wichtige Funktion, wenn Sie Gebühren für den Internet Zugang erheben möchten oder in Situationen, in denen Sie verhindern möchten, dass sich Unbefugte über einen am GuestGate angeschlossenen ungeschützten WLAN Access Point anmelden und Ihren Zugang zum Internet mitbenutzen.

Individuelle Willkommen – Seite für Ihre Gäste

Sie können die Startseite innerhalb von Sekunden ändern. Verändern Sie ganz einfach Inhalt und Formatierung und laden Sie Ihr eigenes Logo hoch. Diese Willkommen-Seite wird angezeigt, wenn sich ein Gast zum ersten Mal mit dem Internet verbinden möchte. Die Willkommen-Seite kann z.B. genutzt werden, damit Gäste Ihren Allgemeinen Geschäftsbedingungen zustimmen müssen. Bei Bedarf kann diese Seite auch deaktiviert werden.



IP PnP

In vielen Situationen ist es notwendig, dass der Netzwerk Administrator die TCP/IP Einstellungen eines Gastcomputers ändert, weil diese nicht mit den vorhandenen Einstellungen des Netzwerkes kompatibel sind oder weitere Einstellungen erforderlich sind. GuestGate beseitigt diesen Schritt vollständig. GuestGate stellt sich automatisch auf die TCP/IP Einstellungen des Gastcomputers ein.

Bandbreitenkontrolle

GuestGate kontrolliert die Verbindungsgeschwindigkeiten jedes angeschlossenen Gastcomputers. Upload und Download Bandbreiten können individuell konfiguriert werden.

Echte Layer 3 Virtual VLAN Funktion

In einem öffentlichen Einsatzort mit einem frei zugänglichen WLAN Access Point ist man oftmals um die Sicherheit besorgt. GuestGate schützt nicht nur Ihr Host Netzwerk vor unbefugten Zugriffen durch Gastcomputer sondern geht noch einen Schritt weiter. Wenn die Option "use separate random network for each client" aktiviert ist, hat kein Gastcomputer Zugriff auf einen anderen Gastcomputer. In diesem Modus teilt GuestGate jedem Gastcomputer ein eigenes, zufällig generiertes Netzwerk zu. Diese Option ist standardmäßig aktiviert.

Packet Filter

Blockiert den Zugriff auf bestimmte Internetseiten oder ganze IP Adressbereiche.

4-Port 10/100 Auto-Sensing LAN Switch

GuestGate bietet vier 10/100 Mbps LAN Switch Ports für den Anschluß von PCs, Notebooks, anderen Switches oder WLAN Access Points.

Webbasiertes Administrator Interface

Die Konfiguration ist komplett Web Browser gestützt. Aus Sicherheitsgründen kann das Administrator Menü nur aus dem Host Netzwerk aufgerufen werden.

Firmware Updates via Web Browser

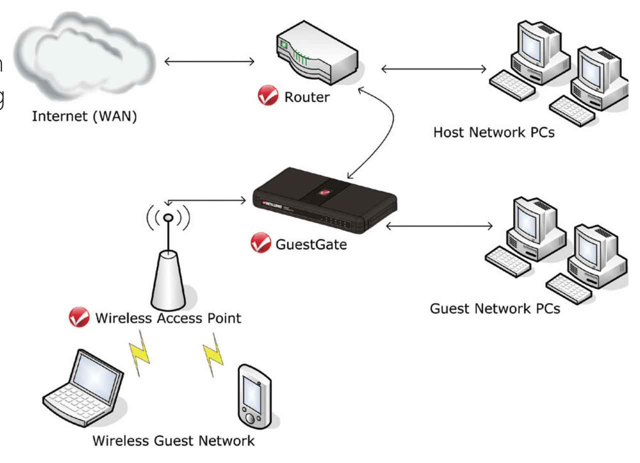
Firmware Updates des GuestGate werden schnell und komfortabel mit dem Web Browser Ihrer Wahl durchgeführt.



INSTALLATIONSBEISPIELE

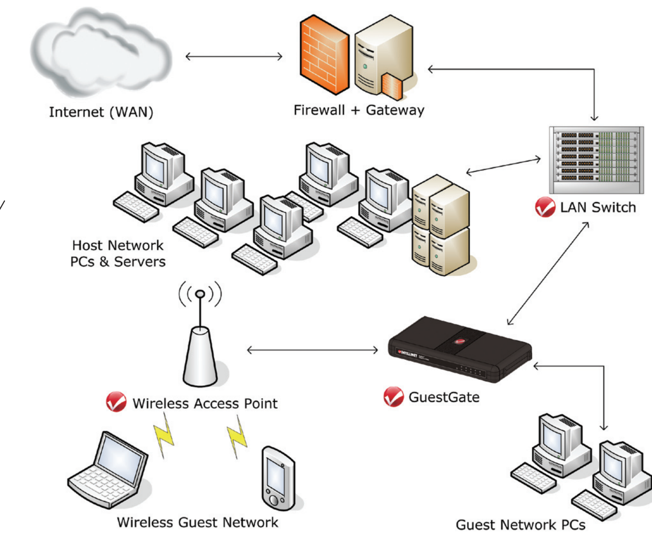
GuestGate innerhalb einer SOHO Netzwerkumgebung

Eine typische Netzwerkumgebung, in der der Internetzugang durch einen NAT Router mit integrierter Firewall zur Verfügung gestellt wird.



GuestGate in einer SMB Netzwerkumgebung

In größeren Netzwerken wird GuestGate mit einem beliebigen Switch verbunden, der sich hinter Firewall/Gateway/ Router befindet.



GUESTGATE BASISFUNKTIONEN

Ports

GuestGate verfügt insgesamt über fünf 10/100 RJ-45 Ports. Mit einem Port wird GuestGate mit dem Host Netzwerk verbunden (Host Port), vier weitere Ports stehen zum Anschluss für Gastcomputer zur Verfügung (Guest Ports). An

die Guest Ports können Hubs, Switches, WLAN Access Points, PCs oder Notebooks angeschlossen werden.

Host (Gastgeber) Ports

Üblicherweise erhält GuestGate eine IP Adresse von einem DHCP Server, der sich im bereits bestehenden Netzwerk befindet. GuestGate analysiert das Netzwerk und erhält alle Informationen die für den Zugang zum Internet notwendig sind. Das DHCP Server Log zeigt die HOST IP Adresse des GuestGate. Für den Fall, dass kein DHCP Server vorhanden ist, wird die IP Adresse des GuestGates standardmäßig auf 192.168.2.1 gesetzt. In diesem Fall ist eine manuelle Konfiguration der HOST IP Einstellungen erforderlich.

Guest (Gast) Ports

GuestGate vergibt IP Adressen an die angeschlossenen Gastcomputer. IP PnP Technologie ermöglicht es, dass keine weitere Konfiguration der Gastcomputer notwendig ist. Der standardmäßige DHCP IP Adressbereich ist 172.16.xxx.xxx. Das Ändern der Gäste-IP Einstellungen ist über das Administrator Menü möglich.

Gast Ports mit Virtual VLAN Funktion

Wenn "Virtual VLAN" aktiviert ist, vergibt GuestGate an jeden angeschlossenen Gastcomputer ein unterschiedliches IP Netzwerk (Subnet). Da diese Einstellungen zufällig generiert werden, ist es für einen Hacker schwierig die IP Einstellungen eines anderen Gastcomputers herauszubekommen um Zugriff zu erhalten. "Virtual VLAN" ist standardmäßig aktiviert, kann jedoch im Guest Konfigurationsmenü des Administrator Menüs deaktiviert werden. Diese Option nennt sich: "separate network for each client (automatic)".

Zugang zum Administrator Web Interface

Die gesamte Konfiguration des GuestGate ist webbasiert. Jeder Standard Web Browser wird unterstützt. Aus Sicherheitsgründen kann das Administrator Menü nur aus dem Host Netzwerk aufgerufen werden. GuestGate lehnt alle Anfragen seitens der Guest Ports ab.

Internet Zugang für Gäste und Willkommen-Seite

Wenn ein Gastcomputer zum ersten Mal versucht auf das Internet zuzugreifen, wird eine Willkommen-Seite im Web Browser angezeigt. Diese Willkommen-Seite kann im Administrator Menü konfiguriert und modifiziert werden. Gäste müssen z.B. Ihren Allgemeinen Geschäftsbedingungen zustimmen, um Zugang zum Internet zu erhalten. Falls die Option Gast Passwort aktiviert ist, muss zunächst ein Passwort eingegeben werden, um Zugriff auf das Internet zu erhalten. Diese Autorisation wird nur einmal benötigt. GuestGate speichert alle autorisierten Gastcomputer, bis er neu gestartet wird. Nach einem Neustart von GuestGate erhalten auch bereits autorisierte Gäste die Willkommen-Seite erneut.



2. INSTALLATION

EMPFOHLENES SETUP

Diese Setup Methode geht davon aus, dass sich ein DHCP Server sowie ein Router in Ihrem Netzwerk befinden.

Anschluss an das Host Netzwerk

Verbinden Sie den HOST Port des GuestGate, mit Hilfe eines RJ-45 Netzwerkkabels, mit einem freien RJ-45 Port in Ihrem vorhandenen Netzwerk (z.B. Ethernet Switch Port, Router Switch Port, etc.). Schalten Sie den GuestGate ein und überprüfen Sie, dass die Netzwerkverbindung aktiv ist (HOST LED am GuestGate muss leuchten). *HINWEIS:* Die Startprozedur kann bis zu 30 Sekunden in Anspruch nehmen.

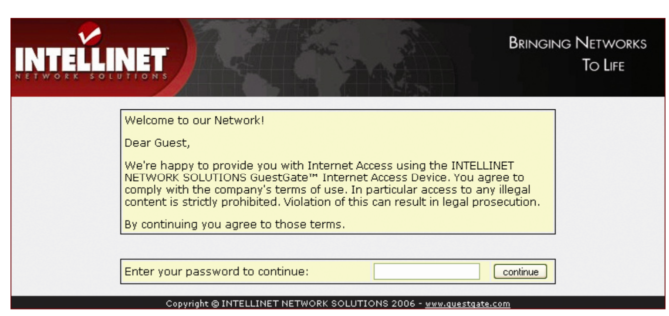
Anschluss von Gastcomputern

Mit Hilfe von RJ-45 Netzwerkkabeln können Sie jetzt PCs, Notebooks, Ethernet Switches, Hubs oder WLAN Access Points an die Guest Ports des GuestGates anschließen. Jeder Port hat seine eigene Status LED. Bitte stellen Sie sicher, dass die Netzwerkverbindung für jeden angeschlossenen Port aktiv ist.

Testen des Internet Zugangs

Starten Sie einen PC oder ein Notebook, welches mit einem Guest Port verbunden ist. Starten Sie einen Web Browser und öffnen Sie eine Internet Seite wie z.B. http://www.intellinet-network.com.

Sie gelangen nun zunächst auf die Willkommen-Seite des GuestGates.



Geben Sie, falls erforderlich, das Passwort ein und klicken Sie auf CONTINUE. Jetzt gelangen Sie auf die Internet Seite, die Sie ursprünglich in der Adresszeile Ihres Web Browsers eingegeben haben.

HINWEIS: Um Zugriff auf das Internet zu erhalten muss zuerst ein Web Browser gestartet und eine Internet Seite aufgerufen werden. Andere Anwendungen wie z.B. Chat Programme (ICQ, MSN Messenger, Skype, etc) haben keine Zugriff auf das Internet, bevor die Willkommen-Seite im Web Browser bestätigt wurde.

Zugriff auf das Administrator Menü aus dem Host Netzwerk

1. Öffnen Sie das Protokoll Ihres DHCP Servers um die IP Adresse Ihres GuestGates herauszufinden. Die MAC (Media Access Control) Adresse des GuestGates finden Sie auf der Unterseite des Gerätes. Mit Hilfe dieser MAC Adresse finden Sie die IP Adresse Ihres GuestGates in der Protokoll-Liste Ihres DHCP Servers. Unten sehen Sie ein Beispiel, wie eine solche Protokoll-Liste eines DHCP Servers aussehen kann:

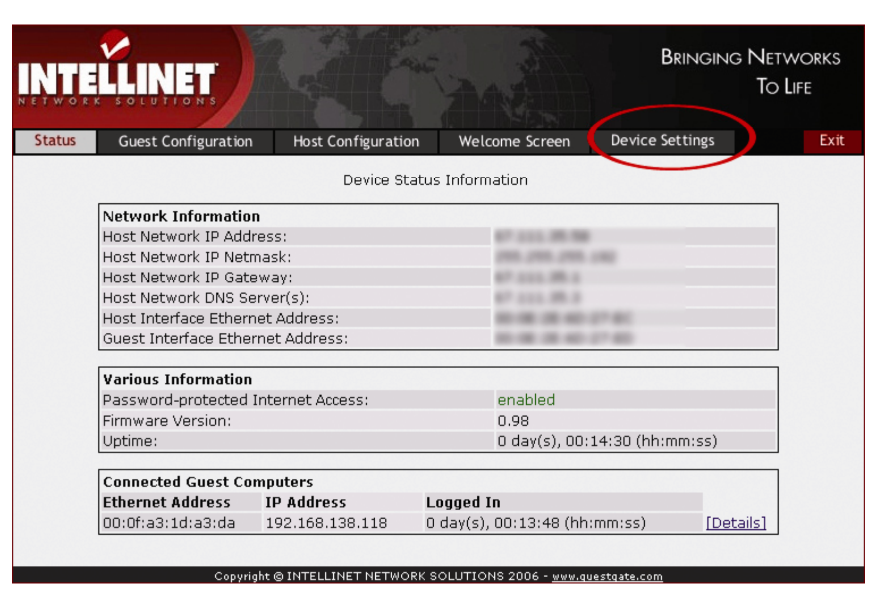
IP Address	MAC Address	Time Expired(s)
192.168.0.100	00:50:fc:be:48:58	169576
192.168.0.101	00:0f:a3:1d:a3:da	114749

2. Starten Sie Ihren Web Browser und öffnen Sie eine Seite mit der IP Adresse aus dem DHCP Protokoll. Als nächstes erscheint das Administrator Web Interface in Ihrem Browser. Das Standard Passwort lautet 1234.

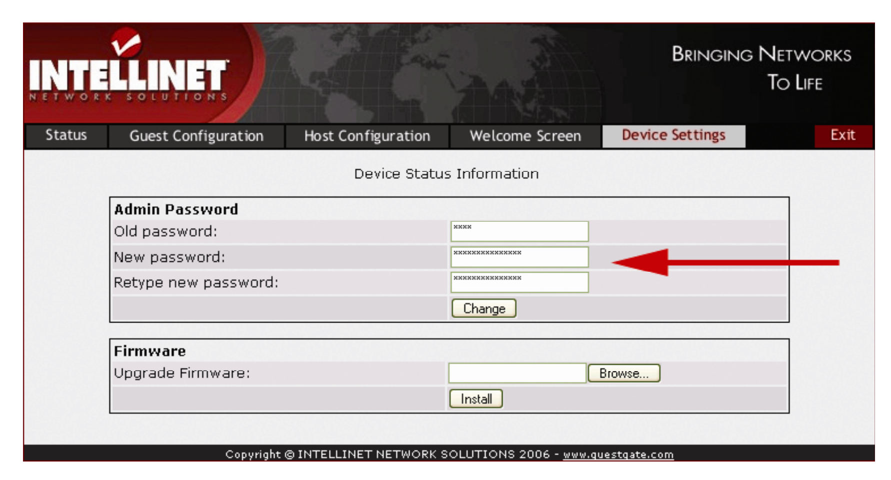


Ändern des Administrator Passwortes

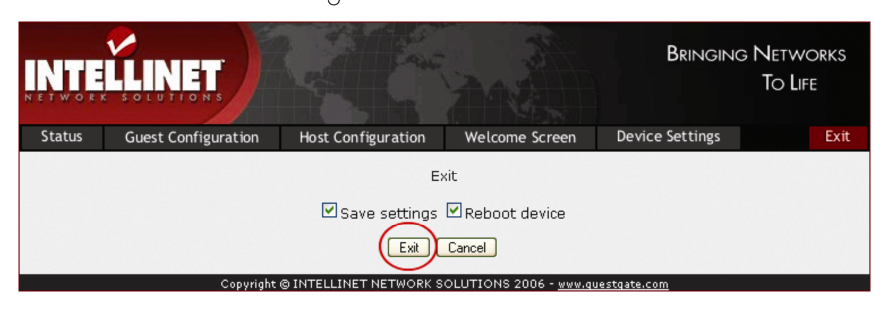
1. Klicken Sie auf "Device Settings."







2. Geben Sie das alte Passwort ein (1234).
3. Geben Sie das neue Passwort ein (bis zu 20 Zeichen lang).
4. Geben Sie erneut das neue Passwort ein.
5. Klicken Sie auf "Exit" (obere rechte Ecke).
6. Aktivieren Sie "Save settings."



7. Aktivieren Sie "Reboot device."
8. Klicken Sie auf "Exit."

Ihr GuestGate führt jetzt einen Neustart durch, dies nimmt etwa 25 Sekunden in Anspruch. Nach dem Neustart werden Sie auf die Login Seite des GuestGates umgeleitet. Sie können sich nun mit dem neuen Passwort einloggen.

HINWEIS: Das Interface wurde so entwickelt, dass Sie in allen 4 Fenstern Änderungen vornehmen können, ohne jedes Mal zu speichern. Erst wenn Sie die Programmierung Ihres GuestGate abgeschlossen haben, müssen Sie auf EXIT und REBOOT klicken. Die Änderungen treten erst nach einem Neustart in Kraft. Wird der Web Browser geschlossen ohne die Konfiguration zu speichern, gehen alle Änderungen verloren.

Wenn Sie alle bisherigen Schritte erfolgreich durchgeführt haben, können Sie das nächste Kapitel "Erweitertes Setup" überspringen.

ERWEITERTES SETUP

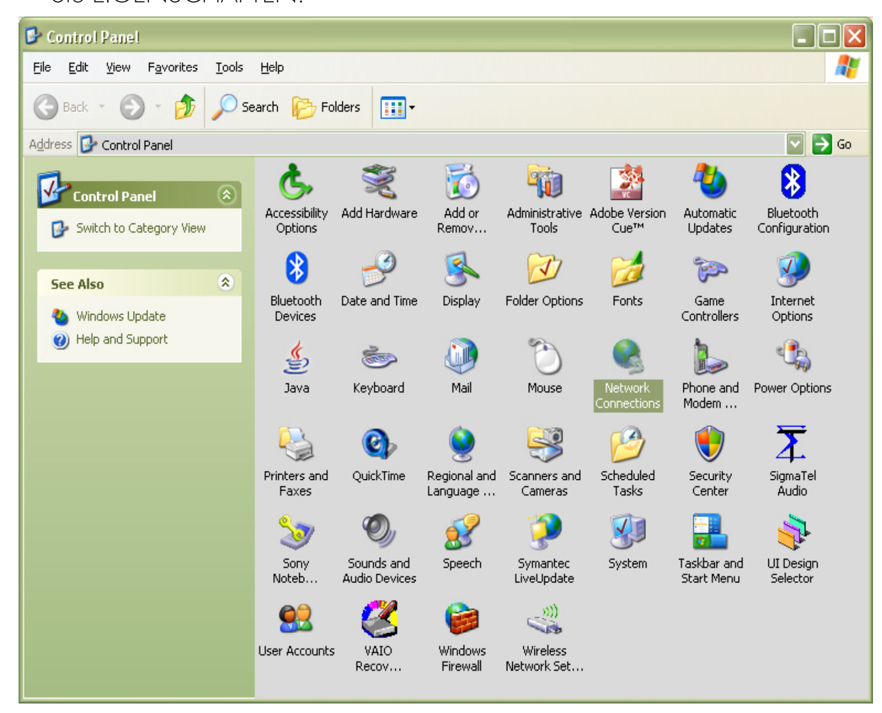
Die Standard Installation des GuestGates geht von der Annahme aus, dass sich ein DHCP Server in Ihrem Netzwerk befindet. Falls dies nicht der Fall ist, können Sie den GuestGate auch manuell konfigurieren. Hierfür schalten Sie den GuestGate ein ohne ihn mit dem Netzwerk zu verbinden. Wenn nnerhalb von 3 Minuten kein DHCP Server gefunden wird, setzt GuestGate seine IP Adresse standardmäßig auf 192.168.2.1.

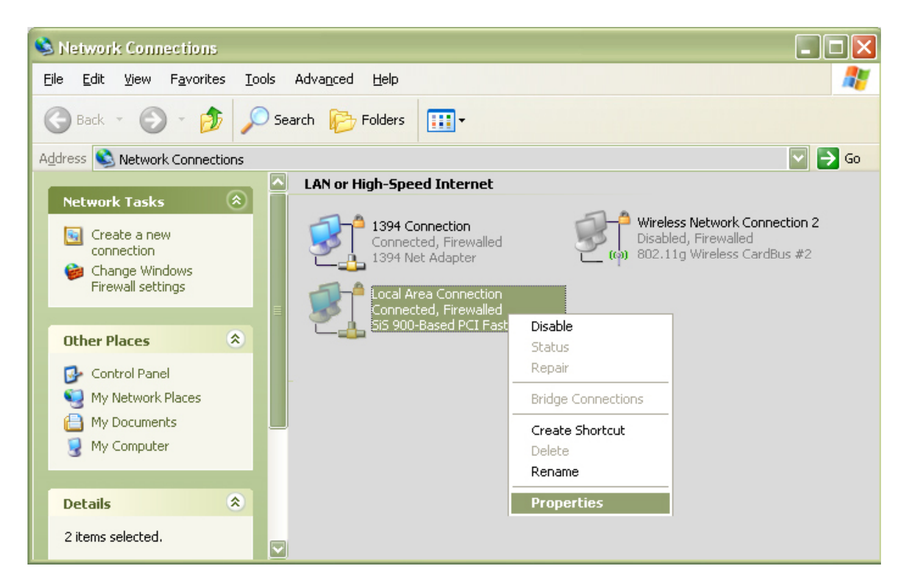
Für das ERWEITERTE SETUP wird folgendes benötigt:

- Ein korrekt eingerichteter Netzwerk Adapter in Ihrem Computer
- Benutzerrechte, die Ihnen erlauben, die TCP/IP Einstellungen an Ihrem PC manuell zu ändern
- GuestGate muss mit einem RJ-45 Netzwerkkabel mit Ihrem Computer verbunden sein

Ändern der IP Adresse Ihres Computers

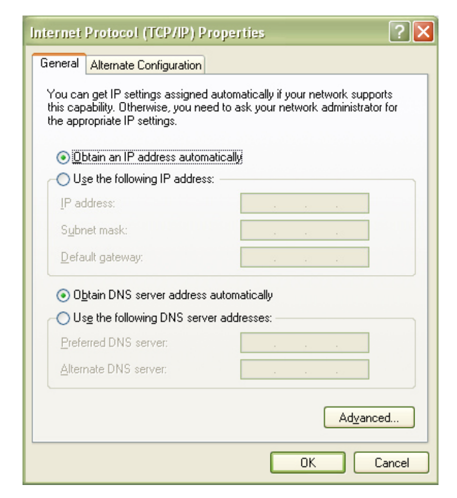
1. Klicken Sie auf START → EINSTELLUNGEN → SYSTEMSTEUERUNG.
2. Doppel-Klick auf NETZWERKVERBINDUNGEN.
3. Drücken Sie mit der rechten Maustaste auf LAN Verbindungen und wählen Sie EIGENSCHAFTEN.

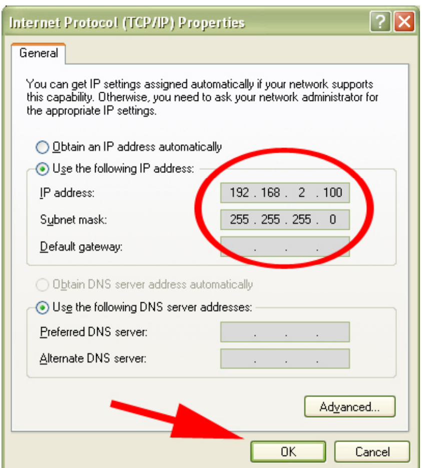




4. In dem neuen Fenster EIGENSCHAFTEN VON LAN VERBINDUNGEN markieren Sie das "Internetprotokoll (TCP/IP)" und klicken dann auf EIGENSCHAFTEN. Wenn sich das Fenster EIGENSCHAFTEN VON INTERNETPROTOKOLL (TCP/IP) führen Sie doe gezeigten Änderungen durch.
5. Wenn Sie fertig sind, klicken Sie auf OK.
6. Schließen Sie das vorherige Fenster, indem Sie ebenfalls auf OK klicken.

Ihre TCP/IP Einstellungen sind jetzt mit denen des GuestGate kompatibel.





Verbinden zum GuestGate via Web Browser

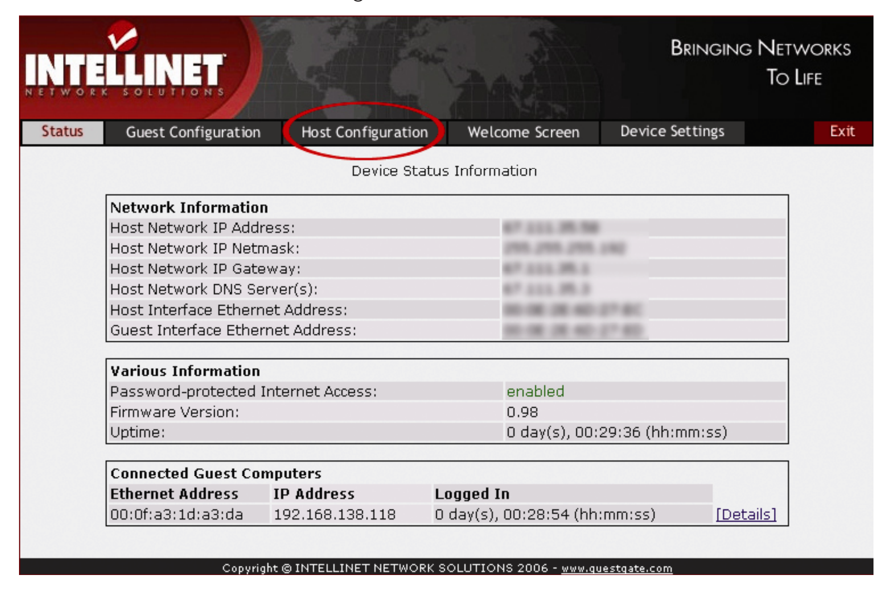
1. Starten Sie Ihren Web Browser und öffnen Sie die Adresse http://192.168.2.1. Der Administrator Web Interface Anmeldebildschirm erscheint nun.
2. Geben Sie das Passwort 1234 ein und klicken Sie auf LOGIN.

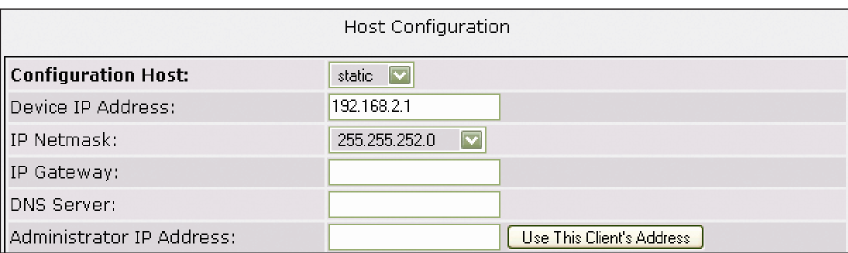


HINWEIS: An dieser Stelle empfehlen wir, das Passwort wie im vorherigen Kapitel beschrieben zu ändern.

Host Konfiguration

1. Klicken Sie auf "Host Configuration."





2. Spezifizieren der IP Adresse, IP Subnetzmaske, des IP Gateways (Internet Verbindungs-Gateway, Router) und DNS Servers.

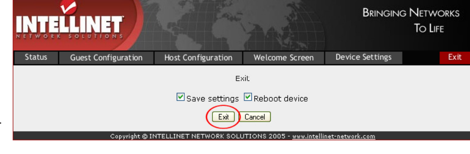
Device IP Address: Hier vergeben Sie die IP Adresse für Ihren GuestGate. Wählen Sie dazu eine in Ihrem Netzwerk noch freie IP Adresse.

IP Netmask: Geben Sie hier die gleiche Subnetzmaske ein, die auch in Ihrem Netzwerk benutzt wird.

IP Gateway: Geben Sie hier die IP Adresse Ihres Internet Gateways ein (z.B. Ihres Routers).

DNS Server: Eingabe der Domain Name Service Serveradresse (wird vom Internetprovider gestellt). Sie können mehrere DNS Server angeben, die Einträge müssen durch ein Leerzeichen getrennt sein.

Administrator IP Address: Wenn angegeben, kann nur von dieser Adresse aus auf das Administrator Menü des GuestGate zugegriffen werden. Durch die Funktion "Use this client's IP Address" wird automatisch die IP Adresse des momentan genutzten Computers in dem Feld hinterlegt.



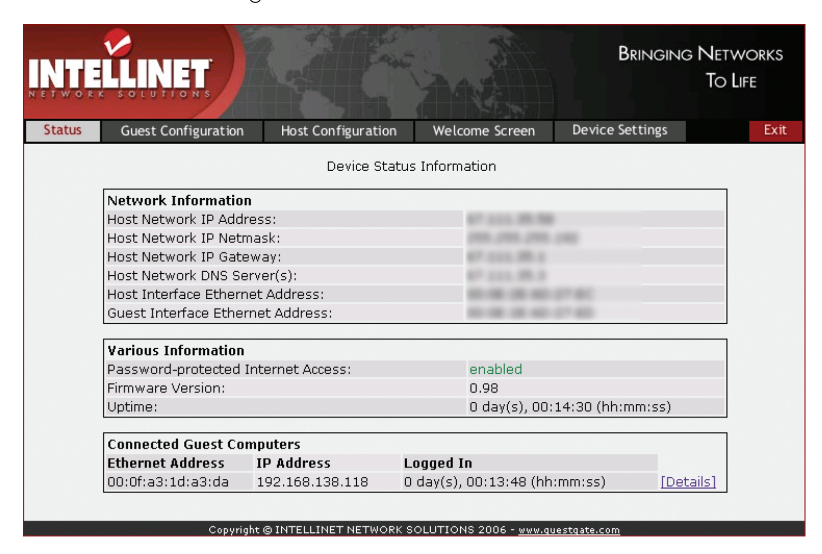
Zum Beenden klicken Sie auf EXIT (obere rechte Ecke).

3. Klicken Sie auf EXIT um die Einstellungen zu speichern und den GuestGate neu zu starten.

3. EINSTELLUNGEN DES GUESTGATE

STATUS BILDSCHIRM

Der Status Bildschirm zeigt drei Arten Informationen:



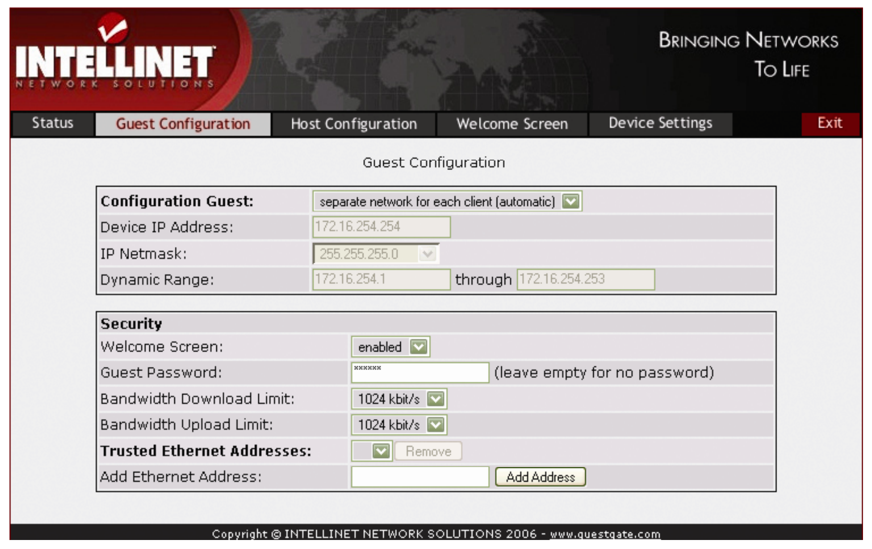
Network Information: Grundlegende Informationen über das HOST Netzwerk.

Various Information: Anzeige der aktuellen Firmware Version, die System Betriebszeit und den Status des Passwortgeschützten Internetzugangs.

Connected Guest Computers: GuestGate führt hier alle angeschlossenen Gastcomputer auf, inklusive deren MAC Adresse, zugewiesener IP Adresse und Anschlusszeit. Klicken Sie auf [Details] um individuelle Statistiken für jeden einzelnen angeschlossenen PC, inklusive verbrauchter Bandbreite (MBytes), zu erhalten.

GAST EINSTELLUNGEN

Diese Seite zeigt die Optionen zur Konfiguration für angeschlossene Gastcomputer.



Configuration Guest

Option "separate network for each client (automatic)": Dieser Betriebsmodus nennt sich "Virtual VLAN". Ist dieser Modus aktiviert, weist GuestGate jedem Gastcomputer ein unterschiedliches, zufällig generiertes Netzwerk zu. Diese Option sollte aktiviert sein, wenn Sie verhindern wollen, dass sich Gastcomputer gegenseitig sehen können oder aufeinander zugreifen können (Virtual VLAN = AN). Diese Option ist standardmäßig aktiviert.

Option "same network for all clients (automatic)": GuestGate weist den Gastcomputern automatisch IP Adressen zu. Alle Gastcomputer arbeiten innerhalb des gleichen Netzwerks (Virtual VLAN = AUS).

Option "same network for all clients (enter manually)": Wird diese Einstellung benutzt, können Sie das Netzwerk für die Gastcomputer manuell bestimmen (Virtual VLAN = AUS).



Welcome Screen

Hier aktivieren bzw. deaktivieren Sie die Willkommen-Seite für Gäste.
Standard = aktiviert.

Guest Password

Wenn Sie Ihre Gäste auffordern möchten, ein Passwort einzugeben, um Zugriff auf das Internet zu bekommen, dann können Sie dieses hier festlegen. Bleibt das Feld leer, wird kein Passwort abgefragt. Standard = kein Passwort.

Bandwidth Download Limit

Einstellen der maximalen Download Bandbreite für angeschlossene Gastcomputer. Einstellungen von 32 kbps (kilo bit per second) bis zu 2048 kbps (= 2 Mega Bit per second) sind möglich. Standard = unbegrenzt.

Bandwidth Upload Limit

Einstellen der maximalen Upload Bandbreite (Senden von Dateien ins Internet), Einstellmöglichkeiten siehe oben.

Trusted Ethernet Addresses

Wenn Sie einen Gastcomputer permantenten Zugriff erlauben möchten, können Sie hier dessen MAC Adresse eingeben. Den Computern in dieser Liste wird keine Willkommen-Seite angezeigt.

Sie finden die MAC Adresse eines angeschlossenen Computers im Status Bildschirm des GuestGate, oder Sie führen folgende Schritte durch (Beispiel: Windows 2000/XP):

1. Klicken Sie auf "Start" → "Ausführen"

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 802.11g Wireless CardBus
        Physical Address. . . . . . . . . : 00-0F-A3-1D-A3-DA
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.10.10.89
        Subnet Mask . . . . . . . . . . . : 255.255.252.0
        Default Gateway . . . . . . . . . : 10.10.8.1
        DHCP Server . . . . . . . . . . . : 10.10.8.10
        DNS Servers . . . . . . . . . . . : 10.10.8.10
                                            10.10.8.21
```

Beispiel

2. Geben Sie ein: cmd; bestätigen Sie mit "Enter."

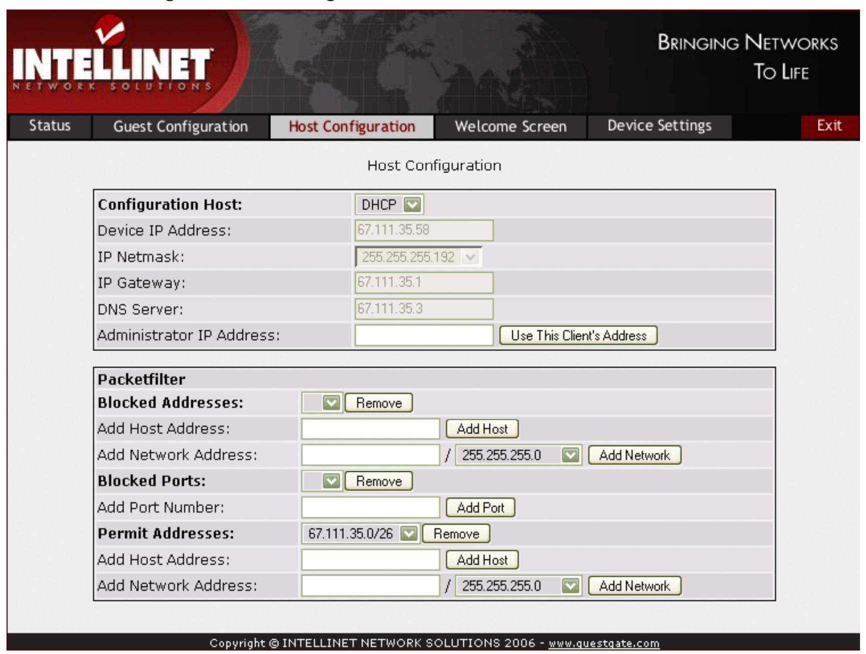
3. Im DOS Fenster geben Sie folgendes ein: "ipconfig /all" und drücken "Enter."

Die PHYSIKALISCHE ADRESSE entspricht der MAC Adresse, welche Sie zur Konfiguration des GuestGate benötigen.

Das richtige Format ist: xx:xx:xx:xx:xx:xx (nicht xx-xx-xx-xx-xx-xx).

HOST EINSTELLUNGEN

Diese Seite zeigt die Einstellungen für den HOST Anschluss des GuestGates.



Configuration Host

Option “DHCP”: GuestGate bekommt automatisch IP Adresse, Subnetzmaske, Gateway und DNS Server Informationen vom DHCP Server in Ihrem Netzwerk zugewiesen, oft handelt es sich hierbei um einen Router. Diese Einstellung ist standard und wird empfohlen.

Option “static”: In größeren Netzwerken kann eine manuelle Konfiguration der IP Einstellungen notwendig sein. Wählen Sie “static” und geben Sie die IP Adresse, Subnetzmaske, Gateway IP Adresse und DNS Server IP Adresse manuell ein

Es können mehrere DNS Server angegeben werden, die durch ein Leerzeichen getrennt werden, z.B. 111.222.333.444 999.888.777.666.

Administrator IP Address: Beschränken Sie den Zugriff auf das Administrator Menu des GuestGate auf die hier angegebene IP Adresse. Es kann sich dabei um eine lokale oder öffentliche IP Adresse handeln.

Packet Filter

Blocked Ports: Wenn Sie bestimmte IP Adressen, Domains oder ein ganzes Netzwerk blockieren möchten, dann können Sie dies hier angeben.



Unter "Add Host Address" können Domänen wie z.B. guestgate.com or intellinet-network.com angeben.

Unter "Add Network Address" können Sie zu blockierende IP Adressen angeben. Um einen ganzen Adressbereich zu blockieren, können Sie die entsprechende Subnetzmaske im Drop Down Menü auswählen.

Blocked Addresses: Hier spezifizieren Sie welche abgehenden TCP/IP Ports Sie blockieren möchten. Geben Sie die Port-Nr. ein und klicken Sie auf "Add Port". GuestGate blockiert sowohl TCP als auch UDP Protokolle.

Eine Liste üblicher Service Ports finden Sie im Kapitel → ANHANG am Ende dieses Handbuchs. Um einen Port zu entfernen, wählen Sie diesen einfach im Drop Down Menü aus und klicken Sie auf "Remove".

HINWEIS: Es können nur einzelne Ports hinzugefügt und entfernt werden.

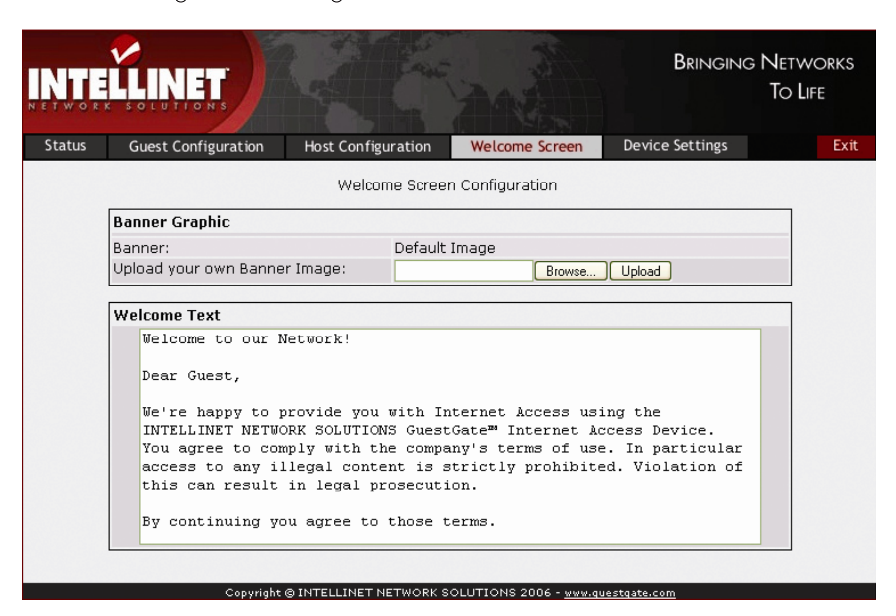
Permitted Addresses: Standardmäßig blockiert GuestGate den Zugriff auf alle PCs auf Seiten des Host Netzwerks. Mit dieser Funktion können Sie Ausnahmen definieren.

Add Host Address: Geben Sie hier eine einzelne IP Adresse ein, z.B. die IP Adresse Ihres Intranet Web Servers und klicken Sie auf ADD HOST. Wiederholen Sie diesen Vorgang, wenn Sie weitere IP Adressen eingeben möchten.

Add Network Address: Geben Sie hier eine IP Adresse und Subnetzmaske ein um einen ganzen IP Adressbereich für Ihre Gäste freizugeben.

WILLKOMMEN BILDSCHIRM

Dese Seiten zeigt die Einstellmöglichkeiten für die Willkommen-Seite des GuestGate.



Banner Graphic

Sie können das Standard Banner durch Ihr eigenes Banner, wie z.B. dem Logo Ihres Unternehmens, ersetzen. Klicken Sie auf Browse um eine Datei zu suchen und auf Upload um diese dann hochzuladen und das Standard Banner zu ersetzen. Nach dem Upload wechselt die Anzeige "Default Image" zu "Custom Image". *HINWEIS:* Der Banner muss folgenden Dateitypen entsprechen: JPG, GIF oder PNG. Die Dateigröße darf 60 Kb nicht überschreiten. Die Abmessungen sind nicht beschränkt, sollten aber idealerweise eine Breite von 1024 Pixel nicht überschreiten. Das Banner wird nur auf der Willkommen-Seite angezeigt. Es ersetzt nicht das Banner im Administrator Menü.

Welcome Text

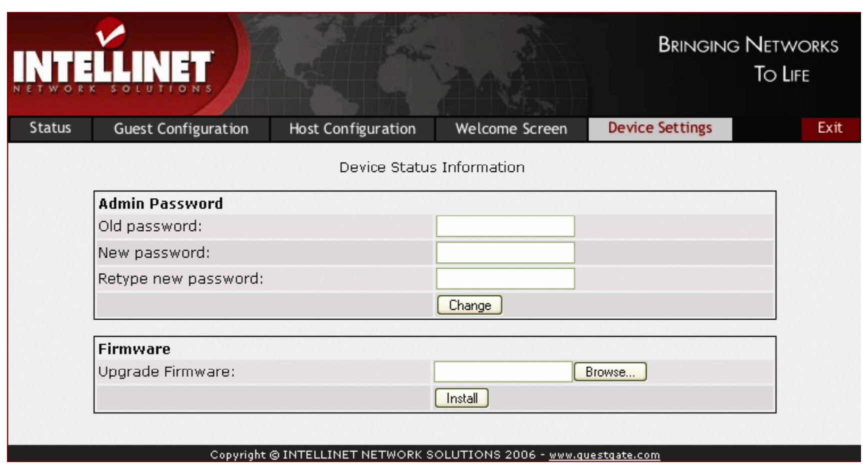
Sie können hier den Standard Text löschen und durch Ihren eigenen Text ersetzen. GuestGate unterstützt HTML tags zum formatieren Ihres Textes. Beispiel:

- **fettgedruckter Text**
- roter Text
- Grüner Text
- <u>unterstrichener Text</u>
- <u>**roter fettgedruckter unterstrichener Text**</u>

Weitere HTML Befehle wie <TABLE> <tr> <td> <img> und viele weitere werden ebenfalls unterstützt.

GERÄT EINSTELLUNGEN

Dieser Bildschirm zeigt die Gerät Einstellungen des GuestGates.





Admin Password

Um das Administrator Passwort zu ändern, müssen Sie zunächst das alte und dann das neue Passwort eingeben. Zur Bestätigung müssen Sie das neue Passwort erneut eingeben. Klicken Sie auf "Change" um die Änderungen zu speichern. Das Standard Passwort des GuestGates lautet 1234. Das Passwort kann eine Länge von bis zu 20 Zeichen haben.

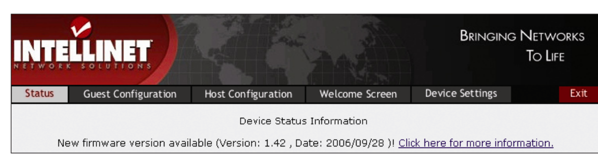
Firmware

Um in Zukunft neue Funktionen nutzen zu können, können Sie die Firmware des GuestGates aktualisieren. Weitere Informationen über den Firmware Update Prozess finden Sie im nächsten Kapitel.

FIRMWARE UPGRADE PROZEDUR

Woher bekommen Sie eine neue Firmware her?

Es gibt zwei Wege herauszufinden, ob eine neue Firmware verfügbar ist.



- GuestGate überprüft, ob eine neue Firmware verfügbar ist, sobald Sie sich im Administrator Menü anmelden. Wenn eine neue Version der Firmware gefunden wird, erscheint eine Mitteilung auf der Status Seite. Klicken Sie auf den Link "Click here for more information" um auf eine Web Seite mit weiteren Details, Anleitungen und der neuen Firmware zu gelangen.
- Gehen Sie in den Download Bereich der Internetseite http://www.guestgate.com.

Upgrade Prozedur

Öffnen Sie den Bildschirm Device Settings des Administrator Menüs.

Klicken Sie auf "Browse" um die neue Firmware auszuwählen, danach klicken Sie auf "Install" um den Upgrade Prozess zu starten. Das Upgrade kann, je nach Verbindungsgeschwindigkeit, einige Minuten in Anspruch nehmen.

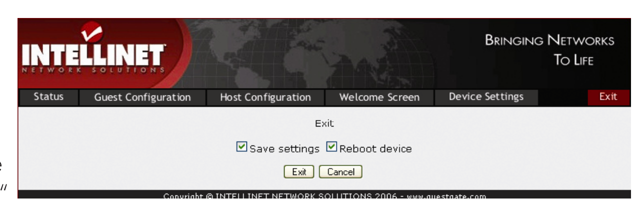
GuestGate führt nach dem Upgrade Prozess automatisch einen Neustart durch. Nachdem Sie die Neustart-Mitteilung gesehen haben dauert es etwa eine Minute, bis Sie wieder auf den GuestGate zugreifen können.

WICHTIG: Der Upgrade Prozess darf nicht unterbrochen werden. Eine Unterbrechung der Netzwerkverbindung oder ein Absturz Ihres Computer während der Upgrade Prozedur kann den GuestGate beschädigen. Idealerweise sollten Sie wenn Möglich das Upgrade aus Ihrem lokalen Host Netzwerk durchführen.

EXIT BILDSCHIRM

In diesem Bildschirm können Sie die aktuelle Konfiguration speichern.

Save Settings



Alle Änderungen die Sie durchgeführt haben werden nur gespeichert, wenn Sie das Feld „Save setting" aktiviert haben. Wenn Sie diesen Schritt nicht durchführen, gehen alle Änderungen die Sie vorgenommen haben beim Schließen des Web Browsers verloren.

Reboot Device

Um die vorgenommenen Änderungen zu übernehmen, müssen Sie dieses Feld aktivieren. *HINWEIS:* Speichern der neuen Einstellungen führt nicht automatisch zu dessen Aktivierung. Es ist notwendig den GuestGate neu zu starten um die neue Konfiguration zu aktivieren. Auf diese Weise können Sie sofort Änderungen vornehmen (z.B. Eingabe eines neuen Gäste Passwortes) und diese erst zu einem späteren Zeitpunkt aktivieren. Ein Neustart des GuestGate erfordert ebenfalls eine erneute Authentifizierung aller angeschlossenen Gastcomputer.

4. FRAGEN & ANTWORTEN

F: Ich habe einen Server in meinem Netzwerk, auf den meine Gäste keinen Zugriff haben sollen. Welche Einstellungen muss ich im GuestGate vornehmen um zu verhindern, dass Gäste auf diesen Server zugreifen können?
A: Sie müssen keine Einstellungen aktivieren. GuestGate unterstützt diese Funktion standardmäßig. Sollte ein Gast versuchen auf einen Server oder Computer in Ihrem Netzwerk zuzugreifen, wird GuestGate dies unterbinden und im Web Browser des Gastcomputers einen Warnhinweis anzeigen.

F: Was, wenn ich meinen Gästen Zugriff auf mein Netzwerk, z.B. meinen Intranet Web Server, erlauben möchte?
A: Geben Sie die IP Adresse Ihres Intranet Servers in den Host Einstellungen des GuestGate im Menüpunkt 'Permit Addresses' an und GuestGate wird den Zugriff auf diesen Server gestatten.

F: Kann ich die Bandbreite der Gastcomputer kontrollieren?
A: Ja. Upload und Download Bandbreiten können in den Gäste Einstellungen des GuestGates im Administrator Menü eingestellt werden.

F: Ich möchte meine eigene Willkommen-Seite anzeigen. Kann ich die ursprüngliche Seite ändern?



A: Ja. Die Willkommen-Seite kann in den Willkommen-Seite Einstellungen des Administrator Menüs geändert werden. Sie können den Text ändern und Ihren eigenen Banner hochladen.

F: Kann ich HTML Code für meine Willkommen-Seite nutzen?

A: Ja. GuestGate schränkt Sie hier in keiner Weise ein. Sie können den HTML Code direkt im Konfigurations-Feld der Willkommen-Seite einfügen.

F: Unterstützt GuestGate PHP, ASP oder Perl?

A: Nein. GuestGate unterstützt keine serverbasierenden Scriptsprachen.

F: Ich habe einige Änderungen im Administrator Menü vorgenommen, diese treten jedoch nicht in Kraft. Warum?

A: Möglicherweise haben Sie vergessen, die neuen Einstellungen auf der EXIT Seite des Administrator Menüs zu speichern.

F: Wofür ist die Option "separate network for each client (automatic)" in den Gäste Einstellungen des GuestGate?

A: Hierbei handelt es sich um die Virtual VLAN Funktion des GuestGate. Wenn diese Option aktiviert ist, verhindert GuestGate durch zufälliges zuweisen von unterschiedlichen TCP/IP Netzwerkeinstellungen an die angeschlossenen Gast computer, dass Gäste sich untereinander 'sehen' können. Auf diese Weise arbeitet jeder Gast in seinem eigenen "Virtual LAN". Die beiden folgenden Beispiele zeigen die Funktionsweise:

1. Gast Einstellungen stehen auf "same network for all clients (automatic)"

   Gastcomputer 1 erhält die IP Adresse 172.16.254.253.
   Gastcomputer 2 erhält die IP Adresse 172.16.254.252.
   Gastcomputer 3 erhält die IP Adresse 172.16.254.251.
   [...]

   In diesem Modus arbeiten alle Gastcomputer in einem Netzwerk und können so gegenseitig aufeinander zugreifen. Dies ist der Standard-Modus von fast jedem üblichen Router und DHCP Server auf dem Markt.

2. Gast Einstellungen stehen auf "separate network for each client (automatic)" (Virtual VLAN aktiviert)

   Gastcomputer 1 erhält die IP Adresse 192.168.17.42.
   Gastcomputer 2 erhält die IP Adresse 172.16.25.12.
   Gastcomputer 3 erhält die IP Adresse 10.10.8.178.
   Gastcomputer 4 erhält die IP Adresse 10.10.4.18.
   Gastcomputer 5 erhält die IP Adresse 192.168.8.178.
   [...]

   In diesem Modus arbeitet jeder Gastcomputer in seinem eigenen Netzwerk und hat deshalb keinen Zugriff auf ein anderes Netzwerk mit Ausnahme des Internets. Da diese Funktion mit zufällig generierten Netzwerken arbeitet, ist es für Angreifer nahezu unmöglich herauszubekommen, welche IP Adresse ein anderer Gast hat. Wenn Sie besorgt um die Sicherheit Ihrer Gäste sind



sollten Sie diese Option aktivieren (Option ist standardmäßig aktiviert).

F: Einige meiner Gäste möchten ein Netzwerkspiel spielen oder Dateien und Verzeichnisse freigeben. Aber das funktioniert nicht. Wie kommt es, dass die angeschlossenen Gastcomputer nicht untereinander kommunizieren können?

A: Das liegt daran, dass standardmäßig Virtual VLAN aktiviert ist. Sie müssen dies zunächst deaktivieren, um eine Kommunikation zwischen den angeschlossenen Gastcomputern zu ermöglichen. (Siehe dazu die verherigeFrage)

F: Wie oft muss ein Gast die Willkommen-Seite bestätigen?

A: Nur einmal. Solange der GuestGate nicht neu gestartet wird, wird der Gast kein weiteres mal aufgefordert, das Passwort einzugeben und Ihren Allgemeinen Geschäftsbedingungen zuzustimmen.

F: Kann ich das Administrator Menü auch von einem Gastcomputer aufrufen?

A: Nein, aus Sicherheitsgründen ist das nicht möglich. Auf das Administrator Menü kann nur über den Host Anschluss zugegriffen werden.

5. SERVICE & SUPPORT

Weitere Informationen über GuestGate finden Sie im Internet unter http://www.guestgate.com/.

Auf dieser Seite
1. finden Sie Antworten auf häufige Fragen (FAQ),
2. erhalten Sie die neueste Firmware Version und
3. können Sie mit unserem technischen Support Team Kontakt aufnehmen.

Im Fall von technischen Problemen empfehlen wir immer zuerst diese Seite zu besuchen, oder kontaktieren Sie Ihren INTELLINET NETWORK SOLUTIONS lieferanten.

6. SPEZIFIKATIONEN

- Host Netzwerk: 1 x 10/100 Mbps RJ-45 Anschluss
- Gast Netzwerk: 4 x 10/100 Mbps RJ-45 Anschlüsse
- Reset Button
- LEDs: 1 x Power, 1 x Link/Activity für das Host Netzwerk, 4 x Link/Activity für die Gäste Anschlüsse
- AC Netzteil 12 V / 0.5 A
- Abmessungen: H: 45 mm, B: 220 mm, T: 120 mm
- Luftfeuchtigkeit: 0 – 90% (nicht kondensierend)
- Temperatur: 10 – 55 °C
- EMI Certification: FCC Class B, CE Mark, C-T



7. ANHANG

Unten finden Sie eine Liste mit oft verwendeten TCP/IP Service Ports. Diese Ports können in den HOST EINSTELLUNGEN des GuestGates eingegeben werden um den Zugriff bestimmter Dienste zu blockieren.

Port Nummer	Dienst/Beshreibung (Hinweis: Diese Liste ist nicht vollständig.)
21	FTP
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Outgoing Mail, Sendmail Server Port)
69	TFTP (Trivial File Transfer Protocol)
70	Gopher
79	Finger
80	HTTP (Standard Web Port for Web Sites)
110	POP3 (Incoming Mail)
115	SFTP (Simple File Transfer Protocol)
119	NNTP (Newsgroups)
123	NTP (Network Time Protocol)
135	RPC service, used for NET SEND command
137, 138, 139	NETBIOS (Filesharing, MS Windows Network)
143	IMAP (Interim Mail Access Protocol)
161	SNMP (Simple Network Management Protocol)
194, 6665-6669	IRC (Internet Relay Chat)
443	HTTS (Secure Web Transfer, used by SSL)
514	SHELL
515	LPR (Line Printer Remote), LPD (Line Printer Daemon)
631	IPP (Internet Printing Protocol)
1080, 3127, 3128, 10080	Trojan: Used by MyDoom
1723	PPTP (used for VPN Connections)
1863	MSN Messenger
2535, 2745, 8866	Trojan: Used by Beagle
3389	Windows XP Remote Desktop Port
3410	Trojan: OptixPro, also used by NetworkLens SSL Event
3689	iTUNES by Apple, DAAP
4899	RADMIN, Remote Control
5000, 5001	YAHOO Messenger Voice Chat
5100	YAHOO Messenger Video (Webcam)
5190, 5191, 5192, 5193	AOL (America On Line via TCP)
5554	Trojan: Sasser Family, also used for SGI ESP HTTP.
5800+, 5900+	VNC
12345	Trojan: Used by Netbus, Italk Chat System and TrendMicro OfficeScan antivirus
27374	Trojan: Used by SubSeven





www.intellinet-network.com

Sind Sie mit diesem Produkt zufrieden?
Bei Fragen oder Kommentaren kontaktieren Sie bitte Ihren
INTELLINET NETWORK SOLUTIONS™ Händler.